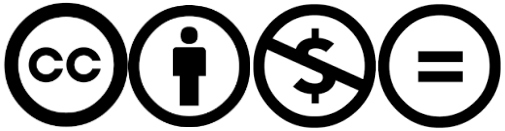
VoIP forensics: un caso pratico di intercettazione

Ing. Vandone Roberto



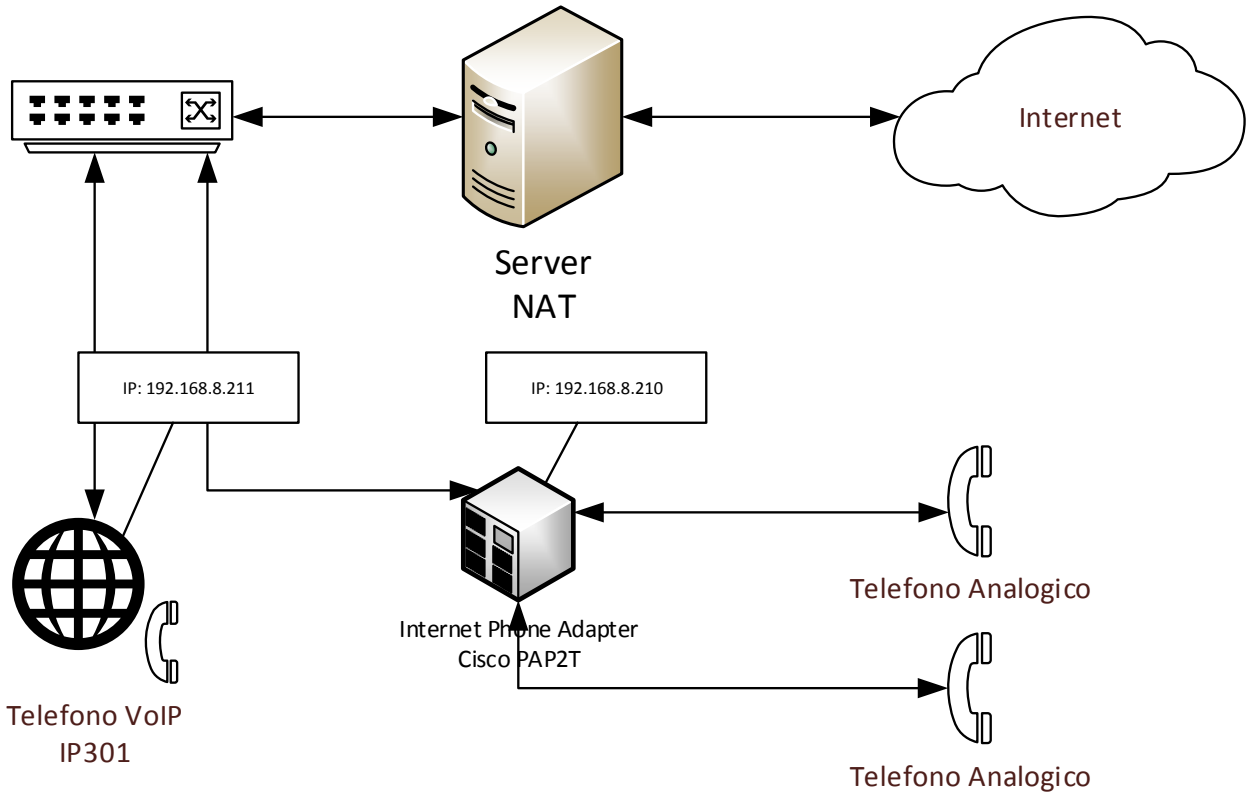
VoIP

- Il VoIP, Voice over IP, identifica una tecnologia che permette di effettuare una conversazione telefonica sfruttando una connessione Internet o, più in generale, una qualsiasi rete dati che utilizzi il protocollo IP.
- Grazie inoltre a numerosi provider VoIP, è possibile effettuare chiamate anche da e verso la rete telefonica tradizionale.

Vantaggi VoIP

- costi inferiori per le chiamate, specialmente sulle lunghe distanze;
- costi contenuti dell'infrastruttura, basta una rete IP;
- possibilità di avere maggiori funzionalità, ad esempio numeri diversi su un unico collegamento;
- salvataggio dei messaggi su PC;
- telefonate gratuite tra utenti dello stesso fornitore o fornitori convenzionati;
- possibilità di implementare un centralino interno utilizzando solo del software;
- possibilità di fare conferenze.
- ……

Topologia rete



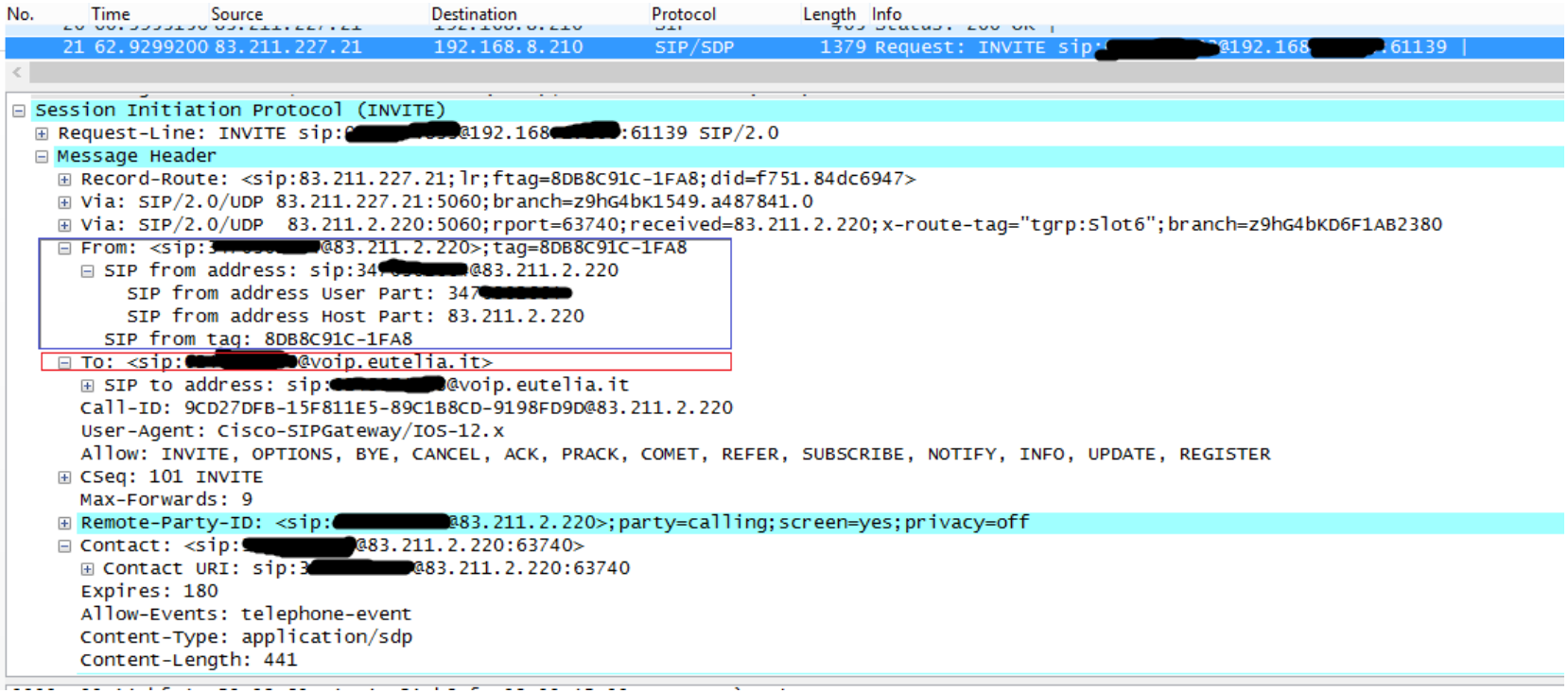
Telefono VoIP IP-301

L'IP 301 è un telefono VoIP molto semplice e diffuso, ha un connettore RJ-45 per permettere il collegamento a Internet e un secondo connettore RJ-45 per permette l'eventuale collegamento diretto ad un PC, infine è presente il connettore per l'alimentazione.

Phone Adapter Cisco PAP2T

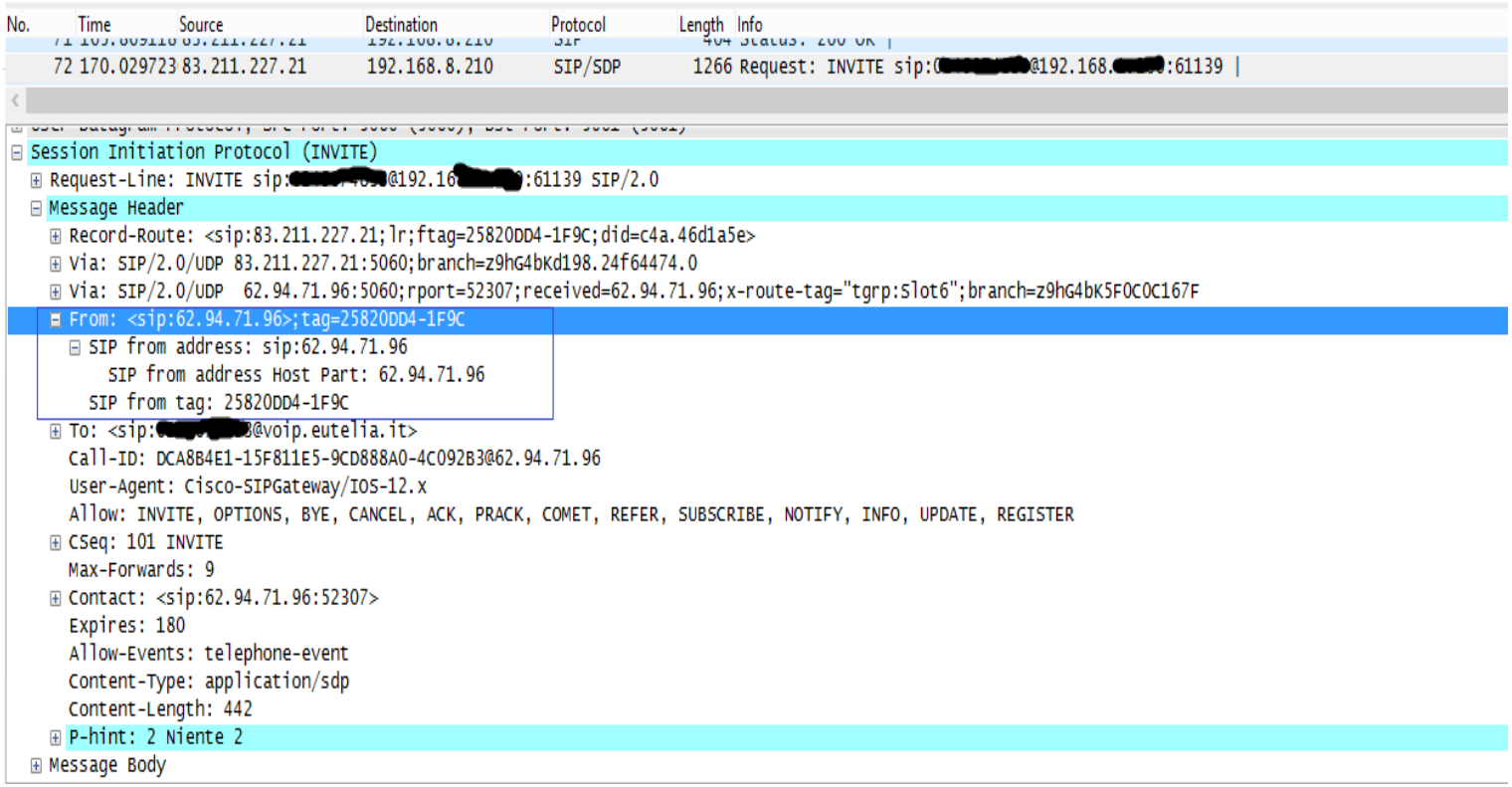
Il PAP2T è un dispositivo economico e molto piccolo, circa 10x10x2,8 cm, ha una porta RJ-45 per il collegamento alla rete, 2 porte RJ-11 per il collegamento ai telefoni analogici e una porta per l'alimentazione. Sono inoltre presenti 4 led che indicano lo stato di funzionamento del dispositivo.

Intercettazione traffico VoIP



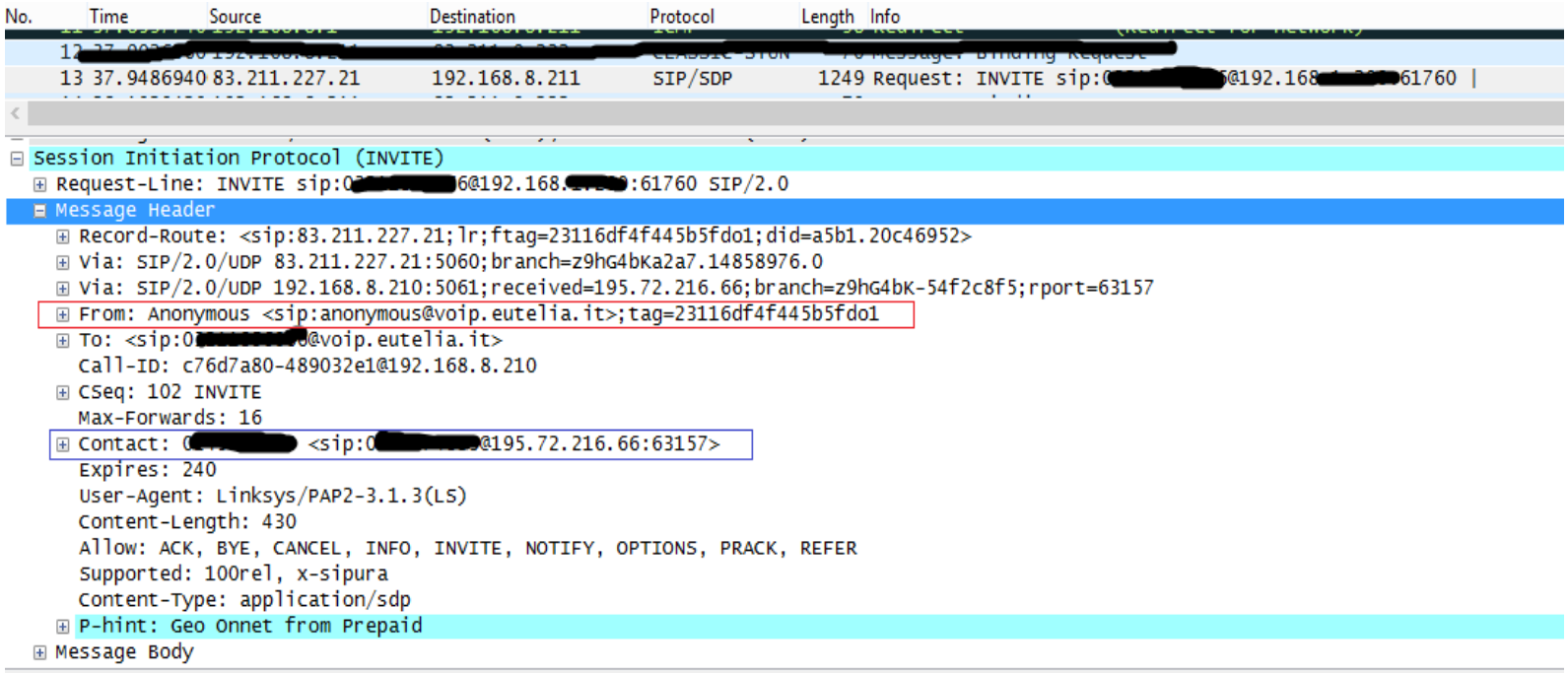
Chiamata da numero esterno

Intercettazione traffico VoIP



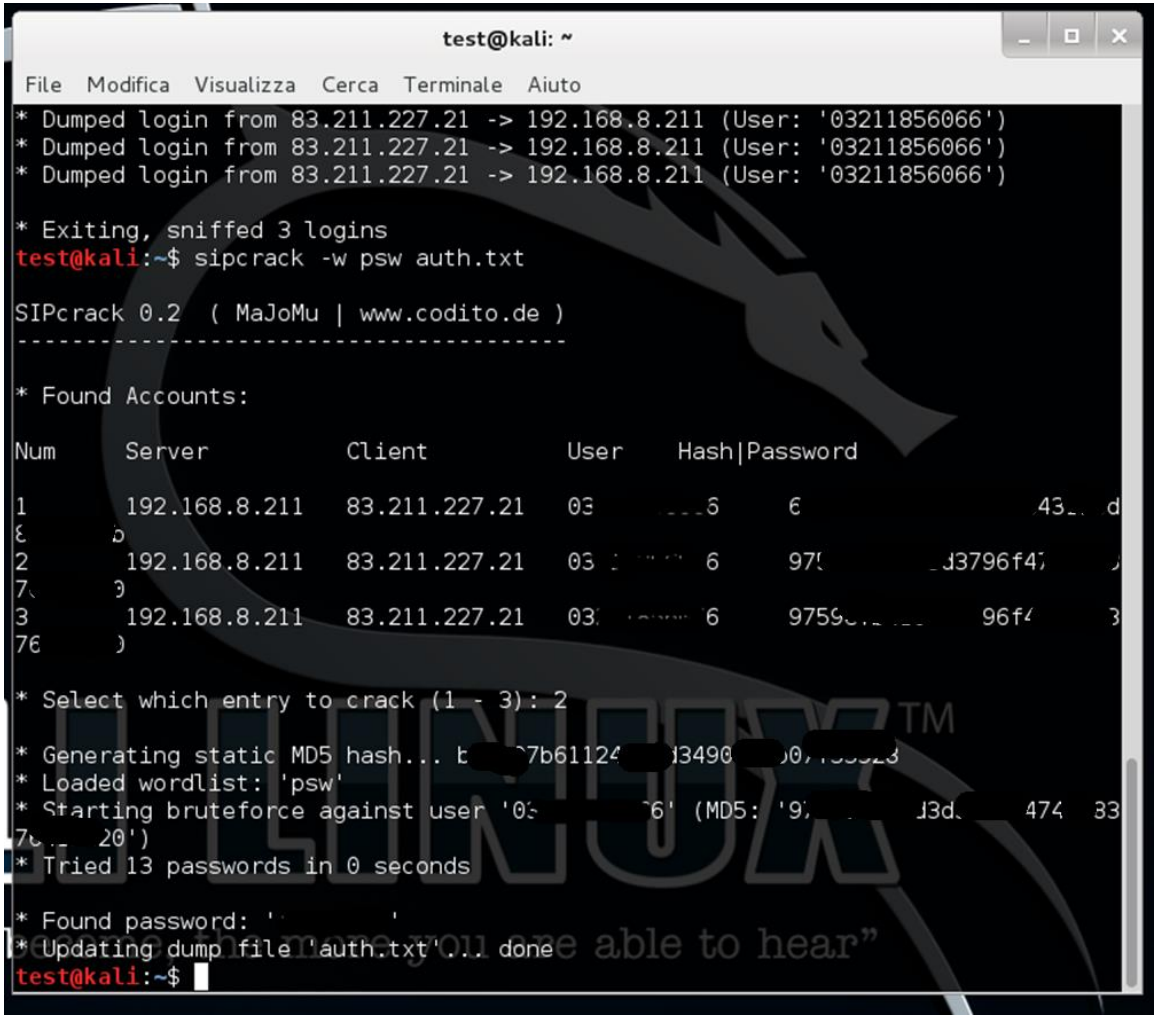
Chiamata da numero nascosto

Intercettazione traffico VoIP

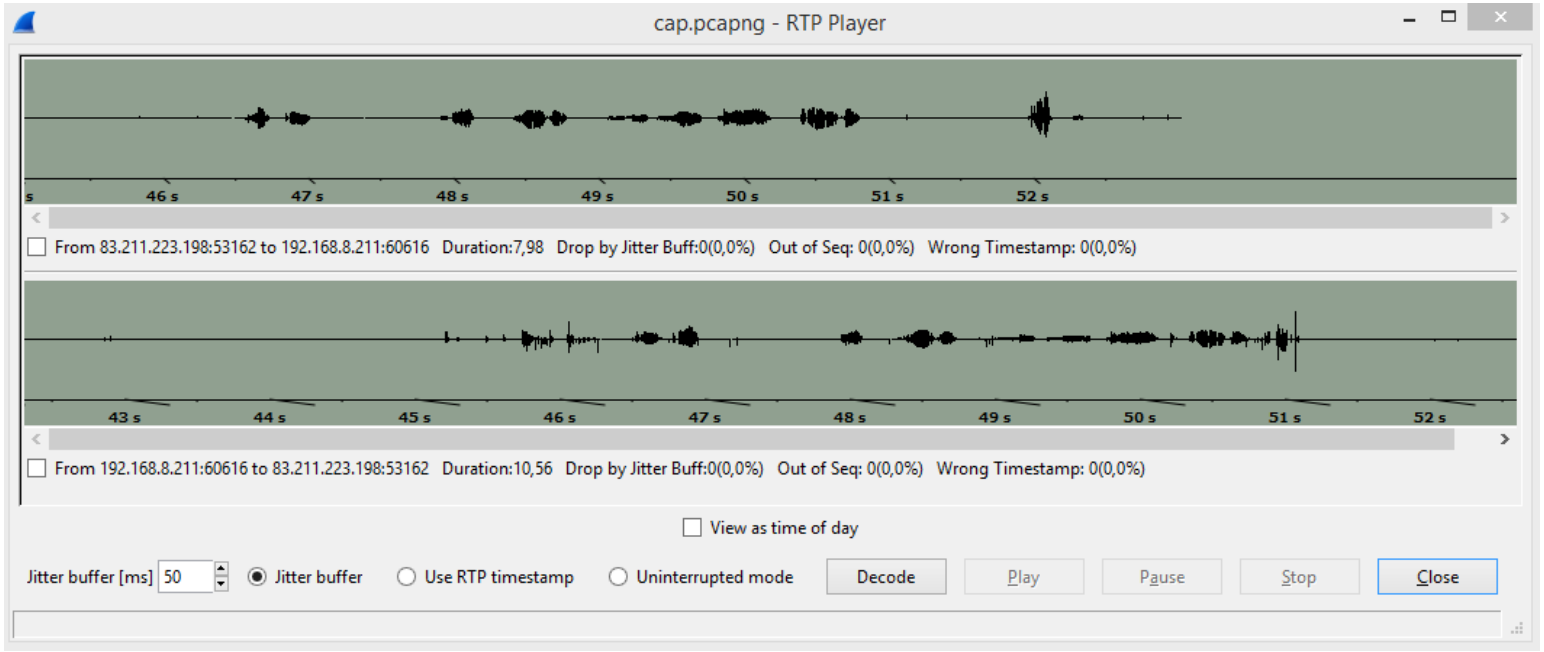


Chiamata da numero nascosto di Eutelia

Intercettazione della password



Intercettazione audio



Conclusioni

- i protocolli SIP e RTP sono molto semplici da analizzare perché in chiaro e si prestano a fornire molteplici elementi utili alle investigazioni.
- è possibile sfruttare le credenziali altrui per «duplicare» un'utenza VoIP.
- trattandosi di dispositivi di rete soffrono inoltre dei problemi classici dei normali device di rete.

Contatti: roberto.vandone@gmail.com